canton de vaud
LIBERTÉ ET PATRIE

Autorité de protection des données et de droit à l'information

Rue Caroline 2
Case postale 171
1001 Lausanne

CHECK-LIST POUR CONTRAT DE SOUS-TRAITANCE DE SOLUTION INFORMATIQUE EXTERNALISÉE

Selon l'art. 18 de la loi du 11 septembre 2007 sur la protection des données personnelles (LPrD ; BLV 172.65), pour pouvoir sous-traiter le traitement de données personnelles, il convient de disposer soit d'une base légale, soit d'un contrat. Dans la plupart des cas, aucune base légale ne prévoit la sous-traitance et la conclusion d'un contrat est dès lors nécessaire. Il est également recommandé de disposer d'un contrat même lorsque la sous-traitance est autorisée par la loi afin de s'assurer du respect des règles de protection des données par le sous-traitant, ainsi qu'en cas de communication transfrontière, garantir un niveau de protection adéquat. Le responsable du traitement (le service métier) qui sous-traite reste entièrement responsable vis-à-vis de la personne concernée du respect de la LPrD.

Le présent document[1] constitue uniquement une aide à la décision et permet de s'assurer que les points principaux ont été prévus dans le contrat. Il est néanmoins important de toujours prendre en compte les spécificités du cas d'espèce. Il ne saurait dès lors être exhaustif.

Questions préalables :

1. Des données personnelles, qu'elles soient sensibles ou non (selon la définition de l'art. 4 al. 1 let. a et b LPrD), seront-elles sous-traitées ?
    a. Non, aucune donnée personnelle ne sera traitée. La LPrD n'est par conséquent pas applicable. Il n'y a dès lors pas besoin de disposer d'un contrat sous l'angle de la protection des données. Il convient néanmoins de disposer d'un contrat pour les autres questions juridiques.
    b. Oui, des données personnelles seront bien sous-traitées. Il convient dès lors de passer au point 2 en lien avec le secret de fonction.

2. Des données personnelles (sensibles ou non) soumises au secret de fonction seront-elles sous-traitées ?
    a. Non, aucune donnée soumise au secret de fonction ne sera traitée. Il n'y a alors pas d'obligation spécifique à respecter en matière de secret de fonction. Il convient néanmoins de disposer d'un contrat pour les autres questions juridiques.
    b. Oui, des données soumises au secret de fonction seront traitées. Il convient alors de prévoir contractuellement que le sous-traitant et ses employés sont soumis au secret de fonction. Le sous-traitant devra également s'assurer du respect effectif du secret par ses employés et par ses sous-traitants en cascade.
        1. Les données soumises au secret de fonction seront-elles traitées en Suisse ?
            a. Oui et il n'y a pas de sous-traitance en cascade à l'étranger. La sous-traitance peut être mise en place (le contrat doit

[1] Le présent document a été élaboré avant l'arrêt Schrems II du 16 juillet 2020 rendu par la Cour de Justice de l'Union européenne (CJUE) lequel invalide la décision d'adéquation 2016/1250 et par là même le dispositif Privacy Shield EU-US.

inclure des règles strictes sur l'interdiction de recourir à des sous-traitants en cascade à l'étranger). Il convient dès lors de passer au point 3 en lien avec le contrat.

b. Oui mais il y a une sous-traitance en cascade à l'étranger (par exemple, sauvegarde ou redondance des données à l'étranger). Il conviendra de chiffrer les données soumises au secret de la manière suivante :
    i. Le chiffrement doit être réalisé en Suisse. La clé de déchiffrement doit, elle, être détenue en Suisse par l'Administration Cantonale Vaudoise (ACV), par le sous-traitant ou par un tiers. Si la clé est détenue par le sous-traitant ou par un tiers, le contrat doit inclure des règles strictes sur l'interdiction de transmettre la clé à l'étranger de manière à ce que les données ne soient déchiffrées.
    ii. Il convient dès lors de passer au point 3 en lien avec le contrat.

c. Non. Il conviendra de chiffrer les données soumises au secret. Le chiffrement doit être réalisé en Suisse et la clé de déchiffrement détenue en Suisse par l'ACV ou par un tiers autre que le sous-traitant. Dans ce dernier cas, le contrat devrait à tout le moins prévoir une interdiction pour le tiers de transmettre la clé de déchiffrement au sous-traitant et une interdiction pour le sous-traitant de tenter de déchiffrer les données. Il convient dès lors de passer au point 3 en lien avec le contrat.

➔ Si ces conditions ne peuvent être respectées, il convient de garder à l'esprit que la transmission de données soumises au secret de fonction et non chiffrées à un tiers prestataire hors de Suisse est susceptible de constituer une violation du secret de fonction (les peines maximales sont la privation de liberté de trois ans au plus ou une peine pécuniaire ; article 320 du code pénal (CP ; RS 311.0).

3. Existe-il un contrat avec le partenaire contractuel ? Dans la majorité des cas, lorsque l'on contracte avec un sous-traitant (notamment dans le cas de fourniture de biens ou de services) un contrat écrit va être établi. Il peut souvent s'agir de conditions générales ou de simples bons de commande.
    a. Oui, un contrat existe. Dans les contrats avec de grandes sociétés, principalement de services informatiques, des clauses de protection des données sont généralement intégrées à leurs conditions générales. Le contrat contient-il des règles de protection des données ?
        i. Non, il n'y a pas de règles de protection des données et il convient de négocier l'intégration de clauses de protection des données
        ii. Oui, il y a des clauses. Sont-elles conformes au regard du projet[2] et suffisantes au regard de la LPrD (cf. ci-après points 4 et suivants) ?
            1. Non, les clauses ne sont pas suffisantes et il convient de les négocier ou d'en ajouter des nouvelles (cf. ci-après points 4 et suivants)
            2. Oui, les clauses sont suffisantes et il n'y a pas d'autres actions à prendre.

[2] En pratique, l'on constate par exemple que certains sous-traitants prévoient dans leurs conditions générales qu'il est interdit d'utiliser le service proposé pour traiter des données sensibles (cf. art. 4 al. 1 ch. 2 LPrD pour la définition) alors que le projet de l'administration tend justement à transmettre des données sensibles au sous-traitant. Il s'agit d'un problème contractuel qu'il convient d'analyser en tout début de projet.

b. Non, il n'y a pas de contrat. Il convient de conclure un contrat portant sur la fourniture de biens ou de services avec le fournisseur et d'y inclure les règles de protection des données (cf. ci-après points 4 et suivants).

Contenu du contrat :

4. Détermination des parties. Les parties au contrat sont-elles suffisamment définies ? Cela est important notamment pour savoir à qui effectivement on sous-traite le traitement de données personnelles.

5. But de la sous-traitance. Il convient de définir le but de la sous-traitance, les données concernées et le cadre dans lequel les données seront transmises. Le sous-traitant ne pourra traiter des données que dans ce cadre.

6. Obligations des parties. Il convient de s'assurer que le sous-traitant s'engage à traiter les données selon les principes généraux de protection des données tels que prévus par la LPrD et selon les instructions du responsable de traitement (le service métier de l'ACV). Le sous-traitant doit notamment s'engager à ne pas utiliser les données dans un autre but que celui communiqué par le responsable de traitement, cela même pour des données pseudonymisées et/ou anonymisées. Le sous-traitant doit s'engager à mettre en place toutes les mesures de sécurité techniques et organisationnelles pour s'assurer de l'intégrité, de la disponibilité et la confidentialité des données et d'informer dans les plus brefs délais le responsable du traitement de tout manquement dans la sécurité des données, de tout accès indu et de toute perte de données. Le sous-traitant devra également informer le responsable du traitement de toute transmission de données à un tiers, même non prévue dans le contrat (par exemple, dans le cas d'une demande officielle comme une autorité judiciaire).

7. La sous-traitance en cascade. La sous-traitance en cascade est-elle autorisée ?
    a. Non, la sous-traitance en cascade n'est pas autorisée et il convient de préciser dans le contrat qu'elle est interdite. Cette solution est dans la mesure du possible à retenir.
    b. Oui, la sous-traitance en cascade est envisageable. Il faut alors prévoir à quelles conditions elle peut être mise en œuvre (accord ou simple information préalable, etc.). Il convient également de prévoir que, sur demande, le sous-traitant s'engage à transmettre au responsable du traitement la liste des sous-traitants en cascade[3]. Il faut encore rappeler que le sous-traitant reste entièrement responsable du respect de la LPrD et de l'éventuel secret de fonction par ses propres sous-traitants.

8. Lieux de traitement des données.
    a. Le traitement des données aura-t-il lieu en Suisse ?
        i. Non, le traitement a lieu à l'étranger. Il faut prévoir que le sous-traitant doive fournir une liste de l'ensemble des pays dans lesquels des données pourront être consultées (par exemple, à des fins de maintenance) et/ou hébergées tant par lui que par ses sous-sous-traitants.
            1. Les données seront traitées dans des pays disposant d'un niveau de protection adéquat (cf. liste) ?
                a. Oui, les données seront traitées dans des pays disposant d'un niveau de protection adéquat et peuvent être communiquées à l'étranger, sous réserve des données soumises au secret de fonction (cf. point 2 ci-dessus)
                b. Non, les données seront traitées dans des pays ne disposant pas d'un niveau de protection adéquat et des garanties supplémentaires doivent être obtenues contractuellement pour

[3] Attention, il convient de vérifier avant de conclure le contrat si de la sous-traitance en cascade est réalisée et, le cas échéant, qui sont les sous-traitants en cascade ainsi que le lieu où ils traitent les données personnelles.

s'assurer que le sous-traitant et ses éventuels sous-traitants respectent les règles de la LPrD (contrat de communication transfrontière de données). Attention aux données soumises au secret de fonction (cf. point 2 ci-dessus).

ii. Oui, le traitement aura lieu en Suisse. Il faut néanmoins prévoir une garantie dans ce sens dans le contrat et s'assurer que les éventuels sous-traitants en cascade traitent les données uniquement en Suisse.

9. Droit de contrôle. Le responsable du traitement doit avoir la possibilité de s'assurer que le sous-traitant (et ses éventuels sous-traitants) respectent bien le contrat et les obligations de protection des données. Il faut notamment pouvoir accéder à tous les documents permettant de vérifier le respect des obligations (journal d'évènements, rapports d'audits, etc.). Un audit doit également pouvoir être mené par le responsable du traitement auprès du sous-traitant et de ses éventuels sous-traitants en cascade. L'autorité de surveillance de la LPrD (APDI) doit aussi avoir la possibilité d'effectuer des contrôles.

10. Droits des personnes concernées. Le sous-traitant doit s'engager à permettre au responsable du traitement de répondre aux demandes formulées par les personnes dont les données sont sous-traitées et à fournir, dans les plus brefs délais, au responsable de traitement toutes les informations et données nécessaires pour répondre à leurs demandes. Il s'agit notamment du droit d'accès à ses propres données[4], du droit de destruction de données illicites, du droit de modification des données, etc. Il doit également s'engager à collaborer avec l'autorité de surveillance de la LPrD (APDI).

11. Responsabilités. Il convient de s'assurer contractuellement que le sous-traitant mette en place les mesures adéquates en lien avec la LPrD pour le traitement des données transmises dans le cadre de la sous-traitance. Il doit également être prévu que le sous-traitant est également responsable pour les faits des sous-traitants en cascade qu'ils soient autorisés ou non. Une indemnisation pleine et entière pour l'ensemble des dommages directs et indirects subis par le responsable du traitement et causés par le sous-traitant ou un sous-traitant en cascade devrait être prévue.

12. Résiliation du contrat. Il convient de prévoir un droit de résilier le contrat par le responsable du traitement, moyennant le respect d'un préavis, sauf dans les cas où de justes motifs (à prévoir dans le contrat ; problèmes graves de sécurité par exemple) permettent de résilier immédiatement le contrat. Les conséquences de la résiliation du contrat doivent être prévues. Il s'agit notamment de l'obligation de restituer dans les plus brefs délais toutes les données au responsable du traitement et de détruire l'ensemble des copies de ces données. Le sous-traitant reste soumis aux règles de la LPrD dans ce cadre. Il est aussi utile de prévoir la transition vers un autre sous-traitant.

13. For et droit applicable. Le droit suisse est-il applicable et un for en Suisse[5] est-il prévu ?
    a. Oui, le droit suisse s'applique et le for est en Suisse. Des données sensibles et des données soumises au secret de fonction peuvent être transmises si les autres conditions sont également remplies (cf. point 2). Il convient dans tous les cas de préférer le droit matériel suisse à un droit étranger.
    b. Non, le droit suisse ne s'applique pas et/ou un for à l'étranger est prévu. Il convient dès lors de ne transmettre des données soumises au secret de fonction que de manière chiffrée selon les modalités du point 2.b. La décision doit être prise par le chef de service. Dans la mesure du possible on essayera d'avoir au moins un for alternatif (par exemple for du défendeur) et l'application du droit matériel suisse.

[4] A noter que le responsable de traitement dispose d'un délai (prévu par la loi) de 30 jours pour répondre aux demandes de droit d'accès qui lui sont adressées.
[5] For exclusif en Suisse romande de préférence.